CFAC Firewall Subcommittee Lead: Jeff Weak

Please submit public comments by 5:00 p.m. MT, Wednesday, June 3rd, 2020, to:

- Jeff.Weak@its.idaho.gov
- CFAC@dfm.idaho.gov

1. Defining what we're purchasing for firewalls

What firewalls do:

- Purchasing two new firewalls that meet our capacity requirements and provide us the latest protection
  - (2) Palo Alto model 7050 firewalls to replace two (2) Palo Alto model 5260's.
- Frontline network security device protecting us from our connection to the public Internet, blocks malicious websites, prevents malware attacks, and prevent a whole range of other cyber-attacks. (It's the one piece of equipment that needs to be refreshed more often to keep up with latest threats)

Why new?

- The current firewalls are maxed with the number of external VPN connections due to COVID
  - The new boxes will meet current and anticipated future demands
- These firewalls are also being placed under far greater loads from agencies taking up more cloud services that are increasing at a very fast pace, includes cloud-based collaboration tools like Microsoft Teams, Zoom, soft phones, etc.
- Our current firewalls have been a major constraint in supporting the work from home order.
  - We fought through *several significant, and long-term network outages.* Streaming video services suffered badly as a result.

2. What is the cost for the firewall component specifically – both the one-time upfront costs and the ongoing costs the state would incur.

- Firewall hardware on-time costs: **$1,062,740**
- Firewall security subscriptions for VPN, Threat Protection, Malware Protection, etc, for 3 years: **$621,600** (to be renewed on year 4)
- Firewall technical support for 3 years: **$241,920** (to be renewed on year 4)
- One-time professional services for installation: **$41,420**
- **Total one-time: $1,104,160**
- **Total 3-year cost: $863,520**
- **Grand Total: $1,967,680**

3. What happens if we don't make this investment and there's a second wave this fall that triggers significant state remote work.

- The reliability and sustainability of the state network will be at high risk of failure and/or incapable of handling the network load
  - We still have staff with compromised immune systems who will continue to telework for the foreseeable future. We need to meet these needs with reasonable accommodations
- There's still no vaccine for COVID. We could be facing a second wave later this year

    - We absolutely must have the infrastructure in place to successfully support another work from home scenario…we can't have infrastructure failing in this situation
- Significant security risk without it
- Bottom line: these firewalls are a massive limiting factor for our network. They're on life-support now under the current load.

---- Additional----

Why firewalls are so important:

***** On 31 Mar we were the target of a significant Distributed Denial of Service (DDoS) attack. The attack knocked our network offline 2 times. At one point in time we had 500,000 network attempts per minute. With the help of our firewall vendor, we created a rule that minimized the effects of the attack. In an eight-hour period the following day, we were targeted 102,000,000 times.